

Harbor - 企业级Docker私有仓库

一 、 安 装 底 层 需 求

**Python**应 该 是 **2.7**或 更 高 版 本

**Docker**引 擎 应 为 **1.10**或 更 高 版 本

**Docker Compose**需 要 为 **1.6.0**或 更 高 版 本

[**docker-compose**](https://github.com/vmware/harbor/releases)： **curl -L** [**https://github.com/docker/compose/releases/download/1.9.0/docker-compose-`uname**](https://github.com/docker/compose/releases/download/1.9.0/docker-compose-`uname) **-s`-`uname -m` > /usr/local/bin/docker-compose**

二 、 **Harbor** 安 装 ： **Harbor** 官 方 地 址 ： [**https://github.com/vmware/harbor/releases**](https://github.com/vmware/harbor/releases)

**1**、 解 压 软 件 包 ： **tar xvf harbor-offline-installer-<version>.tgz**

[**https://github.com/vmware/harbor/releases/download/v1.2.0/harbor-offline-installer-v1.2.0.tgz**](https://github.com/vmware/harbor/releases/download/v1.2.0/harbor-offline-installer-v1.2.0.tgz)

**2**、 配 置 **harbor.cfg**

**a**、 必 选 参 数

**hostname**： 目 标 的 主 机 名 或 者 完 全 限 定 域 名

**ui\_url\_protocol**： **http**或 **https**。 默 认 为 **http**

**db\_password**： 用 于 **db\_auth**的 **MySQL**数 据 库 的 根 密 码 。 更 改 此 密 码 进 行 任 何 生 产 用 途 **max\_job\_workers**： （ 默 认 值 为 **3**） 作 业 服 务 中 的 复 制 工 作 人 员 的 最 大 数 量 。 对 于 每 个 映 像 复 制 作 业 ，

工 作 人 员 将 存 储 库 的 所 有 标 签 同 步 到 远 程 目 标 。 增 加 此 数 字 允 许 系 统 中 更 多 的 并 发 复 制 作 业 。 但 是 ， 由 于 每 个 工 作 人 员 都 会 消 耗 一 定 数 量 的 网 络 **/ CPU / IO**资 源 ， 请 根 据 主 机 的 硬 件 资 源 ， 仔 细 选 择 该 属 性 的 值

**customize\_crt**： （ **on**或 **off**。 默 认 为 **on**） 当 此 属 性 打 开 时 ， **prepare**脚 本 将 为 注 册 表 的 令 牌 的 生 成 **/**验 证 创

建 私 钥 和 根 证 书

**ssl\_cert**： **SSL**证 书 的 路 径 ， 仅 当 协 议 设 置 为 **https**时 才 应 用

**ssl\_cert\_key**： **SSL**密 钥 的 路 径 ， 仅 当 协 议 设 置 为 **https**时 才 应 用

**secretkey\_path** ： 用 于 在 复 制 策 略 中 加 密 或 解 密 远 程 注 册 表 的 密 码 的 密 钥 路 径

**3**、 创 建 **https** 证 书 以 及 配 置 相 关 目 录 权 限

**openssl genrsa -des3 -out server.key 2048**

**openssl req -new -key server.key -out server.csr**

**cp server.key server.key.org**

**openssl rsa -in server.key.org -out server.key**

**openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt**

**mkdir /data/cert**

**chmod -R 777 /data/cert**

**4**、 运 行 脚 本 进 行 安 装

**./install.sh**

**5**、 访 问 测 试

[**https://reg.yourdomain.com**](https://reg.yourdomain.com) 的 管 理 员 门 户 （ 将 **reg.yourdomain.com**更 改 为 您 的 主 机 名 **harbor.cfg**） 。 请 注 意 ， 默 认 管 理 员 用 户 名 **/**密 码 为 **admin / Harbor12345**

**6**、 上 传 镜 像 进 行 上 传 测 试



**a**、 指 定 镜 像 仓 库 地 址

**vim /etc/docker/daemon.json**

**{**

**"insecure-registries": ["serverip"]**

**}**

**b**、 下 载 测 试 镜 像

**docker pull hello-world**

**c**、 给 镜 像 重 新 打 标 签

**docker tag hello-world serverip/hello-world:latest**

**d**、 登 录 进 行 上 传

**docker login serverip**

**7**、 其 它 **Docker** 客 户 端 下 载 测 试

**a**、 指 定 镜 像 仓 库 地 址

**vim /etc/docker/daemon.json**

**{**

**"insecure-registries": ["serverip"]**

**}**

**b**、 下 载 测 试 镜 像

**docker pull serverip/hello-world:latest**

三 、 **Harbor** 原 理 说 明

**1**、 软 件 资 源 介 绍

**Harbor**是 **VMware**公 司 开 源 的 企 业 级 **DockerRegistry** 项 目 ， 项 目 地 址 为 **https://github.com/vmware/harbor** 。 其 目 标 是 帮 助 用 户 迅 速 搭 建 一 个 企 业 级 的 **Dockerregistry**服 务 。 它 以 **Docker**公 司 开 源 的 **registry**为 基 础 ， 提 供 了 管 理 **UI**， 基 于 角 色 的 访 问 控 制 **(Role Based Access Control)**， **AD/LDAP**集 成 、 以 及 审 计 日 志 **(Auditlogging)** 等 企 业 用 户 需 求 的 功 能 ， 同 时 还 原 生 支 持 中 文 。 **Harbor**的 每 个 组 件 都 是 以 **Docker**容 器 的 形 式 构 建 的 ， 使 用 **Docker Compose**来 对 它 进 行 部 署 。 用 于 部 署 **Harbor**的 **Docker Compose**模 板 位 于 **/Deployer/docker-compose.yml**， 由 **5**个 容 器 组 成 ， 这 几 个 容 器 通 过 **Docker link**的 形 式 连 接 在 一 起 ， 在 容 器 之 间 通 过 容 器 名 字 互 相 访 问 。 对 终 端 用 户 而 言 ， 只 需 要 暴 露 **proxy** （ 即 **Nginx**） 的 服 务 端 口

**Proxy**： 由 **Nginx** 服 务 器 构 成 的 反 向 代 理 。

**Registry**： 由 **Docker**官 方 的 开 源 **registry** 镜 像 构 成 的 容 器 实 例 。

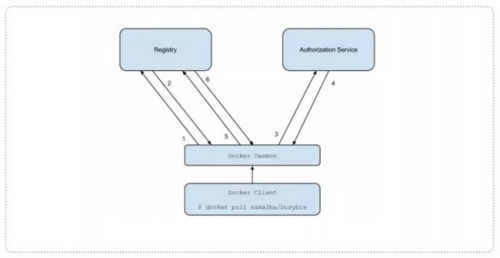
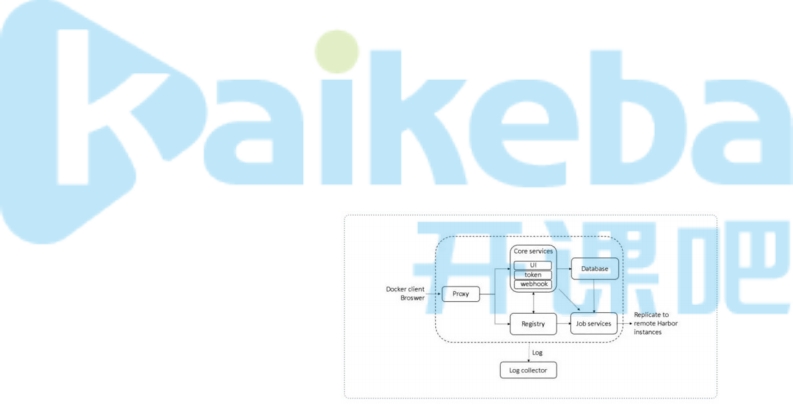
**UI**： 即 架 构 中 的 **core services**， 构 成 此 容 器 的 代 码 是 **Harbor** 项 目 的 主 体 。

**MySQL**： 由 官 方 **MySQL** 镜 像 构 成 的 数 据 库 容 器 。

**Log**： 运 行 着 **rsyslogd** 的 容 器 ， 通 过 **log-driver** 的 形 式 收 集 其 他 容 器 的 日 志

**2**、 **Harbor** 特 性

1. 基 于 角 色 控 制 ： 用 户 和 仓 库 都 是 基 于 项 目 进 行 组 织 的 ， 而 用 户 基 于 项 目 可 以 拥 有 不 同 的 权 限
2. 基 于 镜 像 的 复 制 策 略 ： 镜 像 可 以 在 多 个 **Harbor**实 例 之 间 进 行 复 制
3. 支 持 **LDAP**： **Harbor**的 用 户 授 权 可 以 使 用 已 经 存 在 **LDAP**用 户
4. 镜 像 删 除 **&** 垃 圾 回 收 ： **Image**可 以 被 删 除 并 且 回 收 **Image**占 用 的 空 间 ， 绝 大 部 分 的 用 户 操 作 **API**， 方 便 用 户 对 系 统 进 行 扩 展



1. 用 户 **UI**： 用 户 可 以 轻 松 的 浏 览 、 搜 索 镜 像 仓 库 以 及 对 项 目 进 行 管 理
2. 轻 松 的 部 署 功 能 ： **Harbor**提 供 了 **online**、 **offline**安 装 ， 除 此 之 外 还 提 供 了 **virtualappliance**安 装
3. **Harbor** 和 **docker registry** 关 系 ： **Harbor**实 质 上 是 对 **docker registry** 做 了 封 装 ， 扩 展 了 自 己 的 业 务 模 块

**3**、 **Harbor** 认 证 过 程

1. **dockerdaemon**从 **docker registry**拉 取 镜 像 。
2. 如 果 **dockerregistry**需 要 进 行 授 权 时 ， **registry**将 会 返 回 **401 Unauthorized**响 应 ， 同 时 在 响 应 中 包 含 了 **docker**

**client**如 何 进 行 认 证 的 信 息 。

1. **dockerclient**根 据 **registry**返 回 的 信 息 ， 向 **auth server**发 送 请 求 获 取 认 证 **token**。
2. **auth server**则 根 据 自 己 的 业 务 实 现 去 验 证 提 交 的 用 户 信 息 是 否 存 符 合 业 务 要 求 。
3. 用 户 数 据 仓 库 返 回 用 户 的 相 关 信 息 。
4. **auth server**将 会 根 据 查 询 的 用 户 信 息 ， 生 成 **token**令 牌 ， 以 及 当 前 用 户 所 具 有 的 相 关 权 限 信 息 **.**上 述 就 是 完 整 的 授 权 过 程 **.**当 用 户 完 成 上 述 过 程 以 后 便 可 以 执 行 相 关 的 **pull/push**操 作 。 认 证 信 息 会 每 次 都 带 在 请 求 头 中

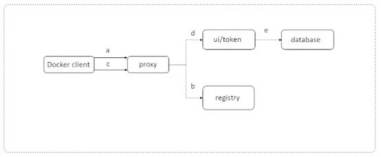
**Harbor**整 体 架 构

**4**、 **Harbor** 认 证 流 程

1. 首 先 ， 请 求 被 代 理 容 器 监 听 拦 截 ， 并 跳 转 到 指 定 的 认 证 服 务 器 。
2. 如 果 认 证 服 务 器 配 置 了 权 限 认 证 ， 则 会 返 回 **401**。 通 知 **dockerclient**在 特 定 的 请 求 中 需 要 带 上 一 个 合 法 的 **token**。 而 认 证 的 逻 辑 地 址 则 指 向 架 构 图 中 的 **core services**。
3. 当 **docker client**接 受 到 错 误 **code**。 **client**就 会 发 送 认 证 请 求 **(**带 有 用 户 名 和 密 码 **)**到 **coreservices**进 行 **basic**

**auth**认 证 。

1. 当 **C**的 请 求 发 送 给 **ngnix**以 后 ， **ngnix**会 根 据 配 置 的 认 证 地 址 将 带 有 用 户 名 和 密 码 的 请 求 发 送 到 **core serivces**。
2. **coreservices**获 取 用 户 名 和 密 码 以 后 对 用 户 信 息 进 行 认 证 **(**自 己 的 数 据 库 或 者 介 入 **LDAP**都 可 以 **)**。 成 功 以 后 ， 返 回 认 证 成 功 的 信 息



**Harbor**认 证 流 程